Oversight Hearing

"No Computer System Left Behind: A Review of the 2005 Federal Computer Security Scorecards"

Thursday, March 16, 2006
10:00 a.m.
Room 2154 Rayburn House Office Building

Opening Statement

Good morning and welcome. A quorum being present, the Committee on Government Reform will come to order. Today, the Committee is releasing its federal computer security scorecards and will examine the status of agency compliance with the Federal Information Security Management Act (FISMA).

Information technology and the Internet drive our economy and help the federal government operate with greater efficiency and cost savings. E-commerce, information sharing, and Internet transactions, such as online tax filing, are so commonplace that we take them for granted. Not until an incident such as the potential Blackberry shutdown – which was recently settled – are we reminded of our dependence on IT and how difficult it is for us to function without it.

In the past year or so, we have heard stories about identity theft, security breaches in large commercial databases, and phishing scams such as those identified by the Internal Revenue Service this tax season. We have also seen an increase in education and awareness campaigns for online safety spearheaded by the private and public sectors. But in my experience, when it comes to *federal* IT policy and information security, it is still difficult to get people – even members of Congress – engaged. For most people this is an abstract, inside-the-Beltway issue. And FISMA is still viewed by some federal agencies as a paperwork exercise. But these are short-sighted observations. As a result of the government's aggressive push to advance e-government, many government information systems hold personal information about citizens and employees, in addition to other types of data. Maintaining the integrity, privacy, and availability of all information in these systems is vital to our national security, continuity of operations, and economy.

Furthermore, in order to successfully fight the war on terror, we must be able to move information to the right people at the right place and time. Information needs to move seamlessly, securely, and efficiently within agencies, across departments, and across jurisdictions of government as well.

Due to the nature of our cyber infrastructure, an attack could originate anywhere at any time. We know that government systems are prime targets for hackers, terrorists, hostile foreign governments, and identity thieves. Malicious or unintended security threats come in varied forms: denial of service attacks, malware, worms and viruses, phishing scams,

and software weaknesses, to name a few. Any of these threats can compromise our information systems. The results would be costly, disruptive, and erode public trust in government.

One of the best ways to defend against attacks is to have a strong, yet flexible, protection policy in place. We want agencies to actively protect their systems instead of just reacting to the latest threat with patches and other responses. FISMA accomplishes this goal by requiring each agency to create a comprehensive risk-based approach to agency-wide information security management. FISMA strengthens Federal cyber preparedness, evaluation, and reporting requirements. It's intended to make security management an integral part of an agency's operations, and to ensure that we are actively using best practices to secure our systems and prevent devastating damage.

The Committee, with technical assistance from GAO, releases annual scorecards based on the FISMA reports submitted to us by agency Chief Information Officers and Inspectors General. This year, the federal government as a whole hardly improved, receiving a D+ yet again. Our analysis reveals that the scores for the Departments of Defense, Homeland Security, Justice, State – the agencies on the front line in the war on terror - remained unacceptably low or dropped precipitously. Meanwhile, several agencies improved their information security or maintained a consistently high level of security from previous years.

The 2005 FISMA grades indicate that agencies have made improvements in developing configuration management plans, employee security training, developing and maintaining an inventory, certifying and accrediting systems, and annual testing. Despite these advances, there are still some areas of concern to the Committee, including implementation of configuration management policies, specialized security training for employees with significant security responsibilities, inconsistent incident reporting, inconsistencies in contingency plan testing, annual testing of security controls, and agency responsibility for contractor systems.

At today's hearing, we will evaluate the results of the agencies' 2005 FISMA reports, identify strengths and weaknesses in government information security, and learn whether FISMA provisions and the OMB guidance are sufficient to help secure government information systems. Witnesses from GAO and OMB will help us understand what obstacles impede the government's ability to comply with FISMA. DOD and DHS witnesses will discuss the challenges they face in their departments and their plans to improve FISMA compliance. We will also hear about best practices and lessons learned from the Social Security Administration and Department of Labor, two agencies that have demonstrated consistent improvements in their information security since the scorecard process was initiated in 2001.

If FISMA was the No Child Left Behind Act, a lot of critical agencies would be on the list of "low performers." None of us would accept D+ grades on our children's report cards. We can't accept these either.